(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平7－182142

(43)公開日　平成７年(1995)７月21日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　7/52		Ａ		

審査請求　未請求　請求項の数４　ＦＤ　（全　７　頁）

(21)出願番号　特願平5－346646

(22)出願日　平成５年(1993)12月22日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

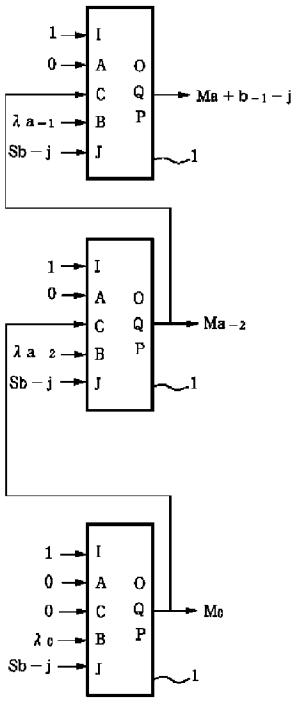
(74)代理人　弁理士　渡部　敏彦

(54)【発明の名称】　多項式乗算回路

(57)【要約】

【目的】　λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供する。

【構成】　本回路は、第１の入力と第２及び第３の入力の積との和を出力する複数の演算素子１をａ個縦に配列したものである。複数の演算素子１を１次元状のアレイで構成することにより、ｘ＾ａ を法としない一般的な多項式の乗算を連続して実行することができ、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える。



1

【特許請求の範囲】

【請求項１】　第１の入力と第２及び第３の入力の積との和を出力する演算素子をａ個配列し、ｉ番目に配列した前記演算素子において、ｉ＋１番目に配列した前記演算素子の出力を前記第１の入力とし、与えられたａ－１次の多項式λ（ｘ）のａ－ｉ次の係数を前記第２の入力とし、与えられたｂ－１次の多項式Ｓ（ｘ）の係数を高次の係数から順次前記第３の入力とすることにより、

Ｍ（ｘ）＝λ（ｘ）・Ｓ（ｘ）

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とする多項式乗算回路。

【請求項２】　ｉ番目の前記演算素子の出力を、

Ｍ（ｘ）＝λ（ｘ）・Ｓ（ｘ）ｍｏｄ Ｘ＾ａ

（ここで“＾”は、その直後の数式が累乗数であることを示している）を展開した多項式のＸ＾ａ-ｉ の係数として得ることを特徴とする請求項１記載の多項式乗算回路。

【請求項３】　第１の入力と第２及び第３の入力の積との和を出力する演算素子をａ個配列し、ｉ番目に配列した前記演算素子において、ｉ＋１番目に配列した前記演算素子の出力を前記第１の入力とし、与えられたａ－１次の多項式λ（ｘ）のｉ－１次の係数を前記第２の入力とし、与えられたｂ－１次の多項式Ｓ（ｘ）の係数を高次の係数から順次前記第３の入力とすることにより、

Ｍ（ｘ）＝λ（ｘ）・Ｓ（ｘ）

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とする多項式乗算回路。

【請求項４】　ｉ番目の前記演算素子の出力を、

Ｍ（ｘ）＝λ（ｘ）・Ｓ（ｘ）／ｘ＾ｂ-2

を展開した多項式の係数として得ることを特徴とする請求項３記載の多項式乗算回路。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は光ディスクや光磁気ディスク等のデータ記憶媒体や、衛生通信等のデータ通信の通信路におけるデータの誤りを訂正するための誤り訂正符号であるリード・ソロモン符号（以下、「ＲＳ符号」と略す。）のような符号処理に好適な多項式乗算回路に関する。

【０００２】

【従来の技術】近年、光ディスク等の記憶媒体を用いたメモリーシステムをはじめとする各種ディジタル・システムの信頼性向上のために、誤り訂正符号を用いた誤り訂正方法の利用が浸透してきている。特に、このような符号としては、ＲＳ符号が、同一の符号長と訂正能力を持つ符号の中で、最も冗長度を小さくできるという実用上重要な特徴を持つため、光ディスクや光磁気ディスク、衛星通信等で広く用いられている。

【０００３】ところで、ＲＳ符号の復号器は、訂正能力が１又は２程度と小さい場合は、比較的容易に装置が構

2

成できるが、訂正能力を大きくした場合、装置の規模が大きくなり、制御も非常に複雑になり、復号処理に要する時間も大きくなってしまうといった問題があった。

【０００４】そこで、並列処理回路の一つであるシストリックアレイを用いた誤り訂正方式が提案されている。それによれば、ＲＳ符号の復号に必要なすべての処理を積和演算ａ・ｂ＋ｃ・ｄに分解し、この演算を同型のプロセッシング・エレメント（ＰＥ）により実行するようにして、このＰＥ１を図６に示すように複数個並べたアレイを利用することにより、多項式λ（ｘ）とＳ（ｘ）のｘ＾ａ を法とする乗算

Ｍ（ｘ）＝λ（ｘ）・Ｓ（ｘ）ｍｏｄ ｘ＾ａ

を簡単な制御により計算し、高速処理が実現されるというものである。なお、図４においてＡ，Ｃ，Ｂ，Ｉ，Ｊ，Ｏ，Ｐ，Ｑは、プロセッシングエレメントを示す。

【０００５】

【発明が解決しようとする課題】しかしながら、上述のシストリックアレイは、λ（ｘ）の係数入力がシリアルに行われる場合に対してのみ有効であり、λ（ｘ）の係数が一括して入力される場合には有効ではなかった。

【０００６】そこで、本発明は、上記事情に鑑みてなされたものであり、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するために請求項１記載の多項式乗算回路は、第１の入力と第２及び第３の入力の積との和を出力する演算素子をａ個配列し、ｉ番目に配列した前記演算素子において、ｉ＋１番目に配列した前記演算素子の出力を前記第１の入力とし、与えられたａ－１次の多項式λ（ｘ）のａ－ｉ次の係数を前記第２の入力とし、与えられたｂ－１次の多項式Ｓ（ｘ）の係数を高次の係数から順次前記第３の入力とすることにより、

Ｍ（ｘ）＝λ（ｘ）・Ｓ（ｘ）

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とするものである。

【０００８】また、請求項２記載の多項式乗算回路は、ｉ番目の前記演算素子の出力を、

Ｍ（ｘ）＝λ（ｘ）・Ｓ（ｘ）ｍｏｄ Ｘ＾ａ

を展開した多項式のＸ＾ａ-ｉ の係数として得ることを特徴とするものである。

【０００９】また、請求項３記載の多項式乗算回路は、第１の入力と第２及び第３の入力の積との和を出力する演算素子をａ個配列し、ｉ番目に配列した前記演算素子において、ｉ＋１番目に配列した前記演算素子の出力を前記第１の入力とし、与えられたａ－１次の多項式λ（ｘ）のｉ－１次の係数を前記第２の入力とし、与えられたｂ－１次の多項式Ｓ（ｘ）の係数を高次の係数から順次前記第３の入力とすることにより、

3

$M(x)=\lambda(x)\cdot S(x)$

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とするものである。

【００１０】また、請求項４記載の多項式乗算回路は、ｉ番目の前記演算素子の出力を、

$M(x)=\lambda(x)\cdot S(x)/x^{b-2}$

を展開した多項式の係数として得ることを特徴とするものである。

【００１１】

【作用】請求項１記載の多項式乗算回路によれば、複数の演算素子を１次元状のアレイで構成することにより、x^a を法としない一般的な多項式の乗算を連続して実行することができ、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える。

【００１２】請求項２記載の多項式乗算回路によれば、複数の演算素子を１次元状のアレイで構成することにより、x^a を法とする多項式の乗算を連続して実行することができ、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える。

【００１３】請求項３記載の多項式乗算回路によれば、複数の演算素子を１次元状のアレイで構成することにより、X^{b-2} での除算を含まない一般的な多項式を連続して実行することができ、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える。

【００１４】請求項４記載の多項式乗算回路によれば、複数の演算素子を１次元状のアレイで構成することにより、X^{b-2} での除算を含む多項式を連続して実行することができ、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える。

【００１５】

【実施例】以下、本発明の実施例を図面を参照して詳述する。

【００１６】図５は本発明の多項式乗算回路を構成する演算素子のブロック構成図である。

【００１７】この演算素子１は、同図に示すように、セレクタ２，第１の乗算器３ａ，第２の乗算器３ｂ，加算器４，第１のレジスタ５ａ，第２のレジスタ５ｂ及び第３のレジスタ５ｃ等から構成される例えばプロセッシング・エレメント（ＰＥ）であり、第１の入力Ｃと第２及び第３の入力Ｂ，Ｊの積との和を出力するものである。また、このセレクタ２は、制御信号Ｓ１，Ｓ2 によって出力端子Ｘに入力Ｃ、出力端子Ｙに入力Ｂを選択するものである。

【００１８】図１は本発明の多項式乗算回路の第１の実施例を示すブロック構成図である。

【００１９】この第１の実施例の回路は、同図に示すように、前記演算素子１をａ個縦に配列し、ｉ番目に配列した演算素子１において、ｉ＋１番目に配列した演算素子１の出力を第１の入力Ｃとし、与えられたａ－１次の多項式λ（ｘ）のａ－ｉ次の係数を第２の入力Ｂとし、

4

与えられたｂ－１次の多項式Ｓ（ｘ）の係数を高次の係数から順次第３の入力Ｊとなるように、各演算素子１間を接続し、x^a を法としない一般的な多項式$M(x)=\lambda(x)\cdot S(x)$ を演算するものである。なお、同図において、ｊは処理クロックを表す。

【００２０】次に、第１の実施例の動作を説明する。

【００２１】ａ－１次の多項式λ（ｘ）のｉ次の計数をλｉ、ｂ－１次の多項式Ｓ（ｘ）のｊ次の係数をＳｊとすると、$M(x)=\lambda(x)\cdot S(x)$ の多項式の乗算は、次のアルゴリズムに示すように、各演算素子１の出力がパイプライン的に次の演算素子１に送られて実行される。但し、Ｍ（ｘ）のｒ次の係数をＭr とし、Mr，Ｚi,j の初期値は０とする。

【００２２】

```
FOR  j＝1  TO  b
   FOR  i＝1  TO  a
      z i,j ＝Zi+1,j-1 ＋λa-1 ・Sb-j
   NEXT
   Ma+b-1-j ＝Zi,j
NEXT
   FOR  i＝2  TO  a
      Ma-i ＝Zi,b
   NEXT
```

この場合、ｉ＋１番目に配列した演算素子１の出力は、処理クロックに同期してｉ番目に配列した演算素子１の第１入力Ｃとしてフィードバック入力される。このとき、Ｍ（ｘ）の高次の係数であるMa+b-1-j （j=1,…，b）は、１番目に配列した演算素子１の出力として順次得られるが、それ以下のＭ（ｘ）の係数Ma-i は、ｂクロック後にｉ番目に配列した演算素子１の出力として一括して得られる。

【００２３】このような第１の実施例によれば、λ（ｘ）の各係数が一括して入力される場合に対して有効な乗算回路が実現できる。また、この回路の制御や構成も全ての演算素子１に対して同じでよいので、規則的で簡単でとなり、ＶＬＳＩに適したものとなる。また、上記の実施例に示した回路は、誤り訂正のためだけに限られず、一般の乗算に対しても有効となる。

【００２４】図２は本発明の多項式乗算回路の第２の実施例を示すブロック構成図である。

【００２５】この第２の実施例の回路は、同図に示すように、第１の実施例と同様に前記演算素子１をａ個縦に配列し、ｉ番目に配列した演算素子１において、ｉ＋１番目に配列した演算素子１の出力を第１の入力Ｃとし、与えられたａ－１次の多項式λ（ｘ）のａ－ｉ次の係数を第２の入力Ｂとし、与えられたｂ－１次の多項式Ｓ（ｘ）の係数を高次の係数から順次第３の入力Ｊとなるように、各演算素子１間を接続し、x^a を法とする多項式$M(x)=\lambda(x)\cdot S(x) \bmod X^a$ を演算するものである。

5

【0026】次に、第2の実施例の動作を説明する。

【0027】a－1次の多項式λ（x）のi次の係数をλi、b－1次の多項式S（x）のj次の係数をSjをとすると、M（x）＝λ（x）・S（x）mod x^aの多項式の乗算は、次のアルゴリズムに示すように、各演算素子1の出力がパイプライン的に次の演算素子1に送られて実行される。但し、M（x）のr次の係数をMr，Zi,jの初期値は0とする。

【0028】

```
FOR  j＝1  TO  b
   FOR  i＝1  TO  a
      Zi,j ＝Zi+1,j-1 ＋λa-i ・Sb-j
   NEXT
NEXT
   FOR  i＝1  TO  a
      Ma-i ＝Zi,b
   NEXT
```

本実施例と第1実施例との違いは、本実施例ではM（x）のa次以上の係数を必要としない、即ち、M（x）mod x^aの演算を実行していることである。第1実施例ではM（x）のa次未満の係数Ma-iはbクロック後にi番目に配列した演算素子1の出力として一括して得られるので、本実施例は図1のi番目に配列した演算素子1の出力をMa-iとして表現している。但し、図2はbクロック後の出力を表し、それまでの図2の回路の動作は図1の回路の動作と同様である。

【0029】図3は本発明の多項式乗算回路の第3の実施例を示すブロック構成図である。

【0030】この第3の実施例の回路は、同図に示すように、第1の実施例と同様に前記演算素子1をa個縦に配列し、i番目に配列した演算素子1において、i＋1番目に配列した演算素子1の出力を第1の入力Cとし、与えられたa－1次の多項式λ（x）のi－1次の係数を第2の入力Bとし、与えられたb－1次の多項式S（x）の係数を高次の係数から順次第3の入力Jとなるように、各演算素子1間を接続し、X^b-2での除算を含まない一般的な多項式M（x）＝λ（x）・S（x）を演算するものである。

【0031】次に、第3の実施例の動作を説明する。

【0032】a－1次の多項式λ（x）のi次の係数をλi，b－1次の多項式S（x）のj次の係数をSjとすると、M（x）＝λ（x）・S（x）の多項式の乗算は、次のアルゴリズムに示すように、各演算素子1の出力がパイプライン的に次の演算素子1に送られて実行される。但し、M（x）のr次の係数をMr とし、Mr,Zi,jの初期値は0とする。

【0033】

6

```
FOR  j＝1  TO  b
   FOR  i＝1  TO  a
     Zi,j ＝Zi+1,j-1 ＋λi-1 ・Sj-1
  NEXT
  Mj-1 ＝Z1,j
NEXT
   FOR  i＝2  TO  a
      Mb-2+i ＝Zi,b
   NEXT
```

この場合、i＋1番目に配列した演算素子1の出力は処理クロックに同期してi番目に配列した演算素子1の第1入力Cとしてフィードバック入力される。このとき、M（x）の低次の係数であるMj-1（j=1，…,b）は、1番目に配列した演算素子1の出力として順次得られるが、それ以上のM（x）の係数であるMb-2+iは、bクロック後にi番目に配列した演算素子1の出力として一括して得られる。

【0034】図4は本発明の多項式乗算回路の第4の実施例を示すブロック構成図である。

【0035】この第3の実施例の回路は、同図に示すように、第1の実施例と同様に前記演算素子1をa個縦に配列し、i番目に配列した演算素子1において、i＋1番目に配列した演算素子1の出力を第1の入力Cとし、与えられたa－1次の多項式λ（x）のi－1次の係数を第2の入力Bとし、与えられたb－1次の多項式S（x）の係数を高次の係数から順次第3の入力Jとなるように、各演算素子1間を接続し、X^b-2での除算を含む多項式M（x）＝λ（x）・S（x）／x^b-2を演算するものである。

【0036】次に、第4の実施例の動作を説明する。

【0037】a－1次の多項式λ（x）のi次の係数をλi、b－1の多項式S（x）のj次の係数をSjとすると、M（x）＝λ（x）・S（x）／xb-2の多項式の乗算は次のアルゴリズムに示すように、各演算素子1の出力がパイプライン的に次の演算素子1に送られて実行される。但し、M（x）のr－1次の係数をMb-2+rとし、Zi,jの初期値は0とする。

【0038】

```
FOR  j＝1  TO  b
   FOR  i＝1  TO  a
      Zi,j ＝Zi+1,j-1 ＋λi-1 ・Sj-1
   NEXT
NEXT
   FOR  i＝1  TO  a
      Mb-2+i ＝Zi,b
   NEXT
```

本実施例と第3実施例との違いは、本実施例ではM（x）のb－2次以下の係数を必要としない、即ち、M（x）／x^b-2の演算を実行していることである。第3実施例ではM（x）のb－1次以上の係数Mb-2+iは

7

ｂクロック後にｉ番目に配列した演算素子１の出力として一括して得られるので、本実施例は図３のｉ番目に配列した演算素子１の出力をMb-2+i として表現している。但し、図４はクロック後の出力を表し、それまでの図４の回路の動作は図３の回路の動作と同様である。

【００３９】なお、本発明は上述した実施例の他、その要旨の範囲内で種々の変形が可能である。例えば、上記各実施例において、演算素子１として図３に示すように汎用性の高いものを用いて、ａ・ｂ＋ｃ・ｄのｄとして１を入力するようにしてａ・ｂ＋ｃの演算を行っているが、初めからこの形の演算を行うような演算素子を用いてもよい。また、各々の演算素子のレジスタ及びセレクタを省略した演算素子を用いてもよい。

【００４０】

【発明の効果】以上詳述した請求項１記載の発明によれば、複数の演算素子を１次元状のアレイで構成したので、ｘ＾ｂ を法としない一般的な多項式の乗算において、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

【００４１】また、請求項２記載の発明によれば、複数の演算素子を１次元状のアレイで構成したので、ｘ＾ｂ を法とする多項式の乗算において、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

【００４２】また、請求項３記載の発明によれば、複数

8

の演算素子を１次元状のアレイで構成したので、Ｘ＾ｂ-２ での除算を含まない一般的な多項式の乗算において、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

【００４３】また、請求項４記載の発明によれば、複数の演算素子を１次元状のアレイで構成したので、Ｘ＾ｂ-２ での除算を含む多項式の乗算において、λ（ｘ）の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

【図面の簡単な説明】

【図１】本発明の多項式乗算回路の第１の実施例を示すブロック構成図である。

【図２】本発明の多項式乗算回路の第２の実施例を示すブロック構成図である。

【図３】本発明の多項式乗算回路の第１の実施例を示すブロック構成図である。

【図４】本発明の多項式乗算回路の第２の実施例を示すブロック構成図である。

【図５】本実施例の演算素子のブロック構成図である。

【図６】従来の多項式乗算回路のブロック構成図である。

【符号の説明】

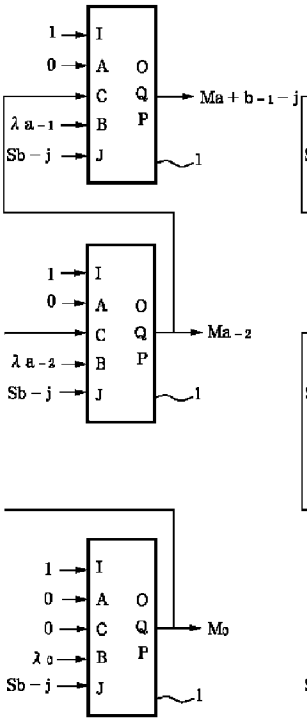
Ｃ　第１の入力

Ｂ　第２の入力

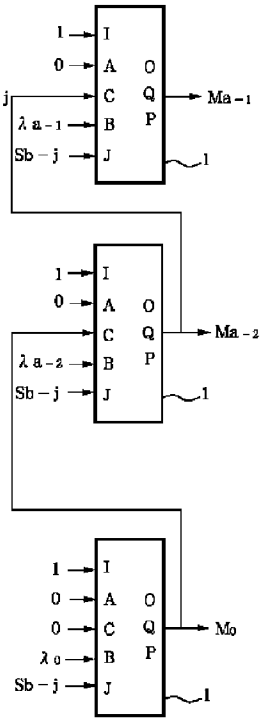
Ｊ　第３の入力

１　演算素子

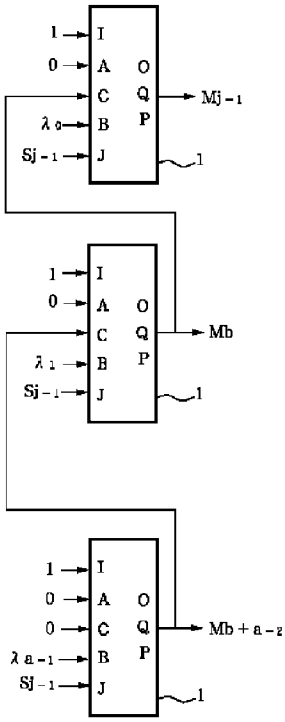
【図１】



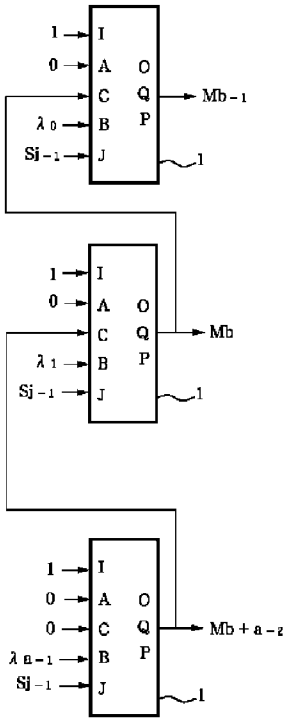
【図２】



【図３】



【図４】



【手続補正書】

【提出日】平成６年６月２０日

【手続補正１】

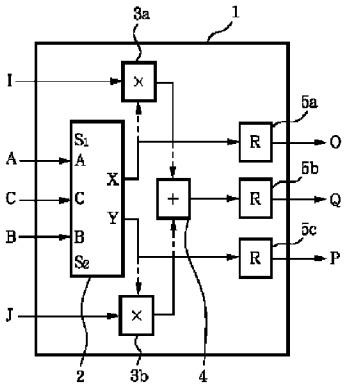
【補正対象書類名】図面

【補正対象項目名】全図

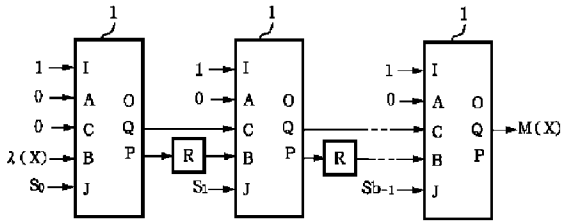
【補正方法】変更

【補正内容】

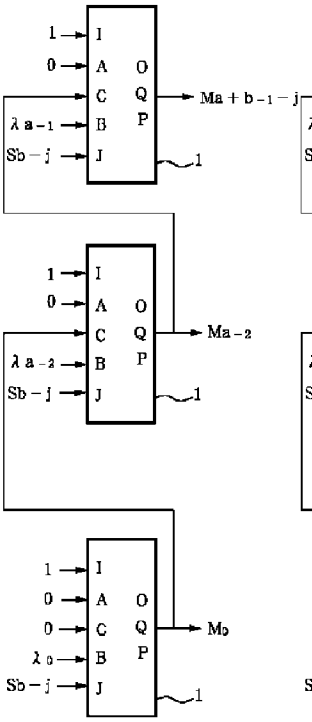
【図５】



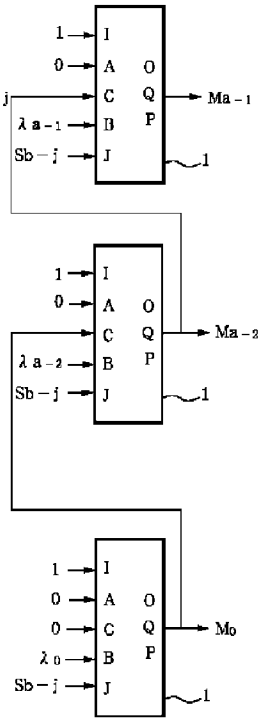
【図６】



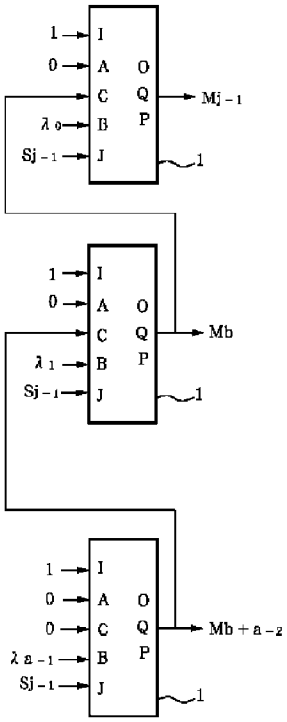
【図１】


1
0
λa−1
Sb−j
I
A
C
B
J
O
Q
P
Ma＋b−1−j
Ma−2
Mo
1

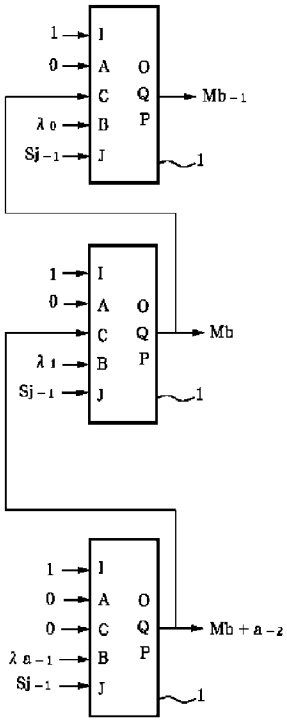
【図２】


1
0
λa−1
Sb−j
I
A
C
B
J
O
Q
P
Ma−1
Ma−2
Mo
1

【図３】


1
0
λ0
Sj−1
I
A
C
B
J
O
Q
P
Mj−1
Mb
Mb＋a−2
1

【図４】


1
0
λ0
Sj−1
I
A
C
B
J
O
Q
P
Mb−1
Mb
Mb＋a−2
1